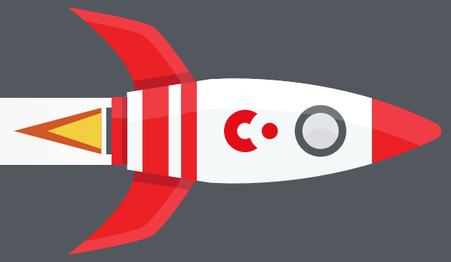
Helping to create a competitive advantage for your CorDapp: upfront compliance by design



So you're building on Corda. And your application addresses an issue or serves to create a better solution in an industry with state, federal or international requirements. In addition, because a customer's auditors may need to get comfortable with the, as they call it, "IT-enabled system" that your CorDapp represents, even the best and most innovative solutions can fail to gain traction if the user community and their procurement, legal and compliance teams can't get comfortable that the application will comply.

That's where System and Organization Controls (SOC) reporting comes into play. The principles embedded in SOC reporting, namely security, availability, processing integrity, confidentiality and privacy, are long established criteria, defined by the American Institute of Certified Public Accountants (AICPA). And when a CorDapp can demonstrate that it can meet hurdles set forth in these principles, by design, they can more readily address concerns from a potential client's compliance team.

When, as a CorDapp developer, you are aware of these needs upfront, you can plan to demonstrate them as you build and document your solution.

What are the 5 Trust Service Principles?

As you build your CorDapp, consider specifically how you can demonstrate it meets the 5 trust principles defined specifically as:

Security
Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.

Availability
Information and systems are available for operation and use to meet the entity's objectives.

Processing integrity
System processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.

Confidentiality
Information designated as confidential is protected to meet the entity's objectives.

Privacy
Personal information is collected, used, retained, disclosed, and disposed to meet the entity's objectives.

What can CorDapp developers do?

It is much more efficient if, upfront, the CorDapp team has a basic understanding of the need to demonstrate these principles. This means fewer headaches when you're confronted with trying to explain or illustrate these by potential customers.

So how do you operationalize this when you're primarily focused on building the best solution? A few considerations:

1. **Educate yourself and your teams:** By reading this article you've already started on the journey! Share it with others and challenge your team to consider where you are now if you had to explain how your CorDapp meets the 5 Trust Principles.
2. **Bake it into your design:** Challenge your design team to bake it into planning and sprints by including the 5 trust principles as a feature check component (i.e. "How does this address security, availability, demonstrate process integrity, impact confidentiality or meet privacy needs?").
3. **Know your customers' industries' unique rules:** Stay current on the key regulations that impact your CorDapp's business model. Illustrating up front for these clients that you understand their regulatory requirements and are able to comply can prove to be a significant competitive advantage, increasing and accelerating adoption.
4. **Ask questions, seek counsel—don't go at it alone:** PwC has resources that can be engaged to assess your organization's readiness to provide a SOC report.
5. **Don't minimize the need to be proactive about the topic:** Avoiding the topic of compliance won't make it go away. And missing out on an important client opportunity because you weren't able to provide documented, standards-based assurance can put your business model at risk.

Interested in learning more? Contact:

Jennifer Lendler, Managing Director
Digital Assurance & Transparency
Emerging Technology, PwC
jennifer.lendler@pwc.com
215-495-4626

Glossary of SOC terms

In case you want a bit more detail, here is a brief explanation of the different types of SOC reports. To consider which one suits your needs, discuss it with a professional. They can align your needs with the right report and also conduct a readiness assessment to determine if you will meet the criteria now if certain changes are made to meet the standard. There is no one size fits all approach but knowing up front that compliance is an issue and working with a certified professional early, will help you navigate.

SOC 1

This report covers the systems and controls at a service organization that may be relevant to an enterprise user's internal controls over financial reporting. It is restricted-use and contains a detailed description of the auditor's testing of controls and the results.

SOC 2

This covers the controls at a service organization relevant to the "trust services principles" which include security, availability, processing integrity, confidentiality, and privacy. Again, this report is restricted-use and contains a detailed description of the auditor's testing of controls and the results.

SOC 3

This general-use report looks at whether a company has maintained effective controls over its system related to the "trust services principles" being reported on. It is similar to a SOC 2 report but excludes the description of the service auditor's testing and results and contains a less detailed description of the service organization's system.

Various Data Regulations

There are many data regulations that affect your CorDapp especially as your CorDapp is used within multiple jurisdictions, various sectors or for government purposes—and they are constantly changing. Here is a summary of just a few:

General Data Protection Regulation (GDPR) is a regulation in the European Union related to data protection and privacy within the EU. It also addresses the transfer of personal data outside the EU.

California Consumer Privacy Act of 2018 (CCPA) was Intended to enhance privacy rights and consumer protection for residents of California by giving consumers more control over the personal information that businesses collect on them.

Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without a patient's consent or knowledge.

Federal Risk and Authorization Management Program (FedRAMP) is a US government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. Security and risk assessment for secure cloud services across the Federal Government. It is a standards approach which is also applied by some businesses in the private sector.

Thus it's important to be sure you're aware and have considered the legal requirements that will impact your CorDapp, your business model and your customer base.

About R3

R3 is an enterprise software firm that is pioneering digital industry transformation. With our foundation in enterprise blockchain technology, we power solutions that deliver trust across the financial services industry and beyond.

R3's enterprise blockchain platform Corda is digitalizing the processes and systems that firms rely on to connect and transact with each other and has more than 350 institutions deploying, servicing and building on it. Our Conclave platform harnesses the promise of confidential computing and Intel® SGX technologies. Conclave empowers businesses to develop applications that analyze and process sensitive data from multiple parties—all without compromising on confidentiality.

Our customers and partners have access to an ecosystem of leading systems integrators, cloud providers, technology firms, software vendors, corporates and banks. To ensure our customers derive the greatest value from their investment, we provide services and support to shorten time-to-market, as well as guidance on implementation, integration and building blockchain business networks. Learn more at r3.com, corda.net, and conclave.net.

About PwC

At PwC, our purpose is to build trust in society and solve important problems. PwC is a network of firms in 155 countries with over 284,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com/US

Continue the conversation

r3.com | corda.net

@inside_r3 | @cordablockchain

r3.com/blog | corda.net/blog

linkedin.com/company/r3cev-llc/